UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

ANDREW J. MORTENSEN, Individually and on Behalf of All Others Similarly Situated,	:	**Case No.**
Plaintiff,	:	**CLASS ACTION COMPLAINT**
-against-	:	
	:	**Jury Trial Demanded**
MARRIOTT INTERNATIONAL, INC.,	:	
Defendant.	:	

Plaintiff Andrew J. Mortensen ("Plaintiff"), for his class action complaint on behalf of himself and all others similarly situated, upon personal knowledge as to the facts pertaining to him and upon information and belief as to all other matters, based on investigation of his counsel, against Defendant Marriott International, Inc. ("Defendant" or "Marriott"), states as follows:

NATURE OF ACTION

This is a consumer class action for damages and injunctive relief against Defendant for damages sustained by Plaintiff and other members of the putative class as a result of Defendant's failure to maintain the security of the financial and personal information disseminated to Defendant in the course of making and purchasing hotel reservations. The type of information which Defendant failed to secure and safeguard is known as personally identifiable information, or PII. Marriott collected such information in connection with the operation of its business as an international hotel chain. Defendant is liable for damages to Plaintiff and the other Class members for inadequate security of Plaintiff's and the other Class members' sensitive personal and financial data against intrusion and breach of security.

INTRODUCTION

1. On November 30, 2018, Marriott disclosed that a data breach lasting four years had compromised the personal information of up to 500 million of its hotel guests worldwide. Marriott said it was first notified of a potential breach on September 8th. Defendant stated it had found that a cache of information had been copied, encrypted, and possibly removed by an unknown hacker. On November 19th, the company was able to decrypt the files and realized the magnitude and nature of the breach. The information stolen includes passport numbers, dates of birth, and potentially credit card information, in addition to contact information such as mailing addresses and email addresses.

2. Marriott's security failures enabled the hackers to steal PII and financial data from Marriott's reservation systems and put Plaintiff's and other Class members' personal and financial information at serious and ongoing risk. The hackers may continue to use the information they obtained as a result of Marriott's inadequate security to exploit and injure Class members across the United States.

3. The Data Breach was caused and enabled by Defendant's knowing violation of its obligations to abide by best practices and industry standards in protecting customers' PII and financial information. Marriott grossly failed to comply with standard security protocols and allowed their customers' personal and financial information to be compromised, all in an effort to save money by cutting corners on security measures that could have prevented or mitigated the Data Breach that occurred.

4. Accordingly, Plaintiff, on behalf of himself and other members of the Class, asserts claims for breach of implied contract and violation of the New York General Business Law § 349 and similar consumer fraud statutes, and seeks injunctive relief, declaratory relief, monetary damages, statutory damages, and all other relief as authorized in equity or by law.

PARTIES

5. Plaintiff Andrew J. Mortensen is a resident of the state of Texas. Plaintiff is a victim of the Data Breach and has suffered damages thereby.

6. Defendant Marriott International, Inc. is a leading global lodging company with more than 6,700 properties across 130 countries and territories, with its principal place of business in Bethesda, Maryland. Marriott is the largest hotel operator in the world.

JURISDICTION AND VENUE

7. This Court has subject matter jurisdiction over this action pursuant to the Class Action Fairness Act of 2005, 28 U.S.C. § 1332(d), because (a) the class has more than 100 members; (b) at least one of the members of the proposed class is a citizen of a state other than New York; and (c) the total amount in controversy exceeds $5 million exclusive of interest and costs.

8. This Court has personal jurisdiction over Defendant because Defendant is authorized to do business in this District, has sufficient minimum contacts with this District, and/or otherwise intentionally avails itself of the markets in this District through the promotion, marketing, and sales in this District so that the exercise of personal jurisdiction of this Court complies with judicial notions of fair play and substantial justice.

9. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(b) because Marriott is subject to this Court's personal jurisdiction.

GENERAL ALLEGATIONS

The Data Breach

10. Like most, if not all, hotel lodging companies, Marriott collects data from its guests during the reservation process. Such data collected includes personally identifiable information, or PII, such as contact information and financial information. When making a reservation at a Marriott

hotel, a Marriott guest develops, maintains, and updates a profile consisting of a large amount of personal information, including the guest's name, address, location, email address, and payment card information. For travel outside the U.S., a Marriott guest must provide passport information, including a passport number. This passport information, together with the personal information listed above, is together referred to herein as "PII."

11. The data stolen during this breach was taken from the Starwood reservation system. Starwood is a hotel company acquired by Marriott in 2016. Starwood properties include W Hotels, St. Regis, Sheraton, Westin, Element, Aloft, the Luxury Collection, Le Meridien, and Four Points. Defendant states the breach affected 500 million guests from an unspecified date in 2014 through September 10th of this year.

12. Marriott stated that the amount of data exposed due to this breach varied from guest to guest. For about 327 million guests, stolen data may have included contact information, passport number, date of birth, gender information, arrival and departure information, reservation date, and Starwood Guest account information. Other guests had less data exposed.

13. An unspecified number of payment card numbers and expiration dates were also exposed. Marriott stated that the card information was encrypted but that the attacker may have obtained the keys to decrypt it.

14. Marriott issued a statement regarding the Data Breach, in which Chief Executive Arne Sorenson stated: "We fell short of what our guests deserve and what we expect of ourselves. We are doing everything we can to support our guests, and using lessons learned to be better moving forward."

15. Marriott's failure to comply with reasonable security standards provided Marriott with short-term and fleeting benefits in the form of saving on the costs of compliance, but at the

expense and to the severe detriment of Marriott's own customers – including plaintiff and Class members here – who have been subject to the Data Breach or otherwise have had their personal and financial information placed at serious and ongoing risk.

16. Marriott allowed widespread and systematic theft of its customers' PII and financial information. Defendant's actions did not come close to meeting the standards of commercially reasonable steps that should be taken to protect customers' personal and financial information.

Security Breaches Lead to Identity Theft

17. The United States Government Accountability Office noted in a June 2007 report on Data Breaches ("GAO Report") that identity thieves use personal identifying data to open financial accounts, receive government benefits, and incur charges and credit in a person's name.[1] As the GAO Report states, this type of identity theft is the most harmful because it may take some time for the victim to become aware of the theft and can adversely impact the victim's credit rating. In addition, the GAO Report states that victims of identity theft will face "substantial costs and inconvenience repairing damage to their credit records . . . [and their] good name."

18. According to the Federal Trade Commission ("FTC"), identity theft requires a number of steps to resolve, including placing a fraud alert and reporting the identity theft to the FTC.[2] Identity thieves use stolen personal and financial information for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.[3]

---

[1] *See* https://www.gao.gov/assets/270/262899.pdf.

[2] *See Identity Theft, A Recovery Plan*, FTC, 1-2 (2016), https://www.consumer.ftc.gov/articles/pdf-0009_identitytheft_a_recovery_plan.pdf (last visited Dec. 4, 2018).

[3] The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority." 16 CFR § 603.2. The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, social security number, date of birth, official State or government issued driver's license or identification number,

19. A person whose personal information has been compromised may not see any signs of identity theft for *years*. According to the GAO Report:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.

The potential for such extensive delays before stolen PII is used necessitates a prolonged vigilance on the part of victims of identity theft. Identity theft victims may need to be "on alert" against illegal use of their PII for years after the data is stolen.

20. PII – such as Marriott's customer names, email addresses, and credit card information that were stolen in the Data Breach at issue in this action – is such a valuable commodity to identity thieves that once the information has been compromised, criminals often trade the information on the "cyber black-market" or "dark web" for a number of years.[4] As a result of recent large-scale data breaches, identity thieves and cyber criminals have openly posted stolen credit card numbers, and other PII directly on various Internet websites making the information publicly available.

21. This information can be sold on the black market or dark web almost immediately. Speaking about the infamous 2017 Equifax data breach, Justin Shipe, vice president of information security at CardConnect, a payment processor, stated: "Once [your personal information is] out there, it's out there."[5]

---

alien registration number, government passport number, employer or taxpayer identification number." *Id*.

[4] Companies, in fact, also recognize PII as an extremely valuable commodity akin to a form of personal property. *See* John T. Soma, J. Z. Courson & John Cadkin, ET AL, *Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets*, 15 RICH. J.L. & TECH. 11, at *3-4 (2009).

[5] Brian Fung, *You can pretty much assume someone has your data. What to do next.*, CHI. TRIB., (Sep. 21, 2017, 10:08 AM), http://www.chicagotribune.com/business/ct-identity-theft-

22. Identity thieves can combine PII from the Marriott Breach to "fill in the blanks" for victims of earlier breaches where some additional information was still needed.

23. Moreover, this card information can be worth as much as $45 on the black market, according to the New York Times reporting on the Target data breach:

> The black market for credit card and debit card numbers is highly sophisticated, with numerous card-selling sites that are indistinguishable from a modern-day e-commerce site. Many sell cards in bulk to account for the possibility of cancellations. Some go for as little as a quarter apiece. Corporate cards can sell for as much as $45.[6]

The Monetary Value of Privacy Protections

24. At an FTC public workshop in 2001, then-Commissioner Orson Swindle described the value of a consumer's personal information as follows:

> The use of third party information from public records, information aggregators and even competitors for marketing has become a major facilitator of our retail economy. Even [Federal Reserve] Chairman [Alan] Greenspan suggested here some time ago that it's something on the order of the life blood, the free flow of information.[7]

25. Though Commissioner Swindle's remarks are more than a decade old, they are even more relevant today, as consumers' personal data functions as a "new form of currency" that supports a $26 billion per year online advertising industry in the United States.[8] For example,

---

protection-20170921-story.html.

[6] Elizabeth A. Harris, *In Apology, and a Sale, Target Tries to Appease*, N.Y. Times (Dec. 20, 2013), https://www.nytimes.com/2013/12/21/business/in-apology-and-a-sale-target-tries-to-appease.html.

[7] *The Information Marketplace: Merging and Exchanging Consumer Data*, FTC, Mar. 13, 2001, https://www.ftc.gov/sites/default/files/documents/public_events/information-marketplace-merging-and-exchanging-consumer-data/transcript.pdf.

[8] Julia Angwin & Emily Steel, *Web's Hot New Commodity: Privacy*, THE WALL STREET JOURNAL (Feb. 28, 2011, 12:01 AM), https://www.wsj.com/articles/SB10001424052748703529004576160764037920274.

supermarket operator Kroger Co. records what customers buy at its more than 2,600 stores. Then, Kroger sifts through this data and sells that information for upwards of $100 million annually.[9]

26. As the FTC recognizes, once identity thieves have personal information, "they can drain your bank account, run up charges on your credit cards, open new utility accounts, or get medical treatment on your health insurance."[10]

27. Personal and financial information such as that stolen in the Marriott Data Breach is highly coveted by and a frequent target of hackers. Legitimate organizations and the criminal underground alike recognize the value of such data. Otherwise, they would not pay for or maintain it, or aggressively seek it. Criminals seek personal and financial information of consumers because they can use such data to perpetuate more and larger thefts. The stolen PII can be used to gain access to an assortment of existing accounts and websites.

28. The ramifications of Defendant's failure to keep customer's personal and financial information secure are severe. Identity theft occurs when someone uses another's personal and financial information such as that person's name, credit card number, credit card expiration dates, and other information, without permission, to commit fraud or other crimes.

29. Identity thieves can use personal information, such as that pertaining to the Plaintiff and the Class, which Marriott failed to keep secure, to perpetuate a variety of crimes that harm the victims. The United States government and privacy experts acknowledge that it may take years for identity theft to come to light and be detected.

30. Identity thieves can also use stolen PII to harm victims through blackmail, embarrassment, or harassment in person or online, or to defraud victims by obtaining ID cards or

[9] Vipal Monga, *What Is All That Data Worth?*, THE WALL STREET JOURNAL (Oct. 13, 2014), http://asia.wsj.com/documents/print/WSJ_-B001-20141013.pdf.
[10] *Warning Signs of Identity Theft*, FTC (May 2015),

driver's licenses, fraudulently obtaining tax returns and refunds, and obtaining government benefits. Identity theft can be time-consuming and costly to its victims, as a 2007 Presidential Report detailed:

> Individual victims . . . collectively spend billions of dollars recovering from the effects [of identity theft].
>
> In addition to the losses that result when identity thieves fraudulently open accounts or misuse existing accounts, . . . individual victims often suffer indirect financial costs, including the costs incurred in both civil litigation initiated by creditors and in overcoming the many obstacles they face in obtaining or retaining credit. Victims of non-financial identity theft, for example, health-related or criminal record fraud, face other types of harm and frustration.
>
> In addition to out-of-pocket expenses that can reach thousands of dollars for the victims of new account identity theft, and the emotional toll identity theft can take, some victims have to spend what can be a considerable amount of time to repair the damage caused by the identity thieves. Victims of new account identity theft, for example, must correct fraudulent information in their credit reports and monitor their reports for future inaccuracies, close existing bank accounts and open new ones, and dispute charges with individual creditors.11

31. Consumers place a high value not only on their PII, but also on the *privacy* of that data. Researchers have shed light on how much consumers value their data privacy – and the amount is considerable. Indeed, studies confirm that "when [retailers'] privacy information is made more salient and accessible, some consumers are willing to pay a premium to purchase from privacy protective websites."[12]

---

https://www.consumer.ftc.gov/articles/0271-warning-signs-identity-theft.

[11] The President's Identity Theft Task Force, *Combating Identity Theft: A Strategic Plan*, FTC, 11 (April 2007), https://www.ftc.gov/sites/default/files/documents/reports/combating-identity-theft-strategic-plan/strategicplan.pdf (last visited Dec. 4, 2018).

[12] Janice Y. Tsai & Serge Egelman & Lorrie Cranor & Alessandro Acquisti, *The Effect of Online Privacy Information on Purchasing Behavior: An Experimental Study*, 22(2) INFORMATION SYSTEMS RESEARCH 254, 254 (June 2011).

32. Given these facts, any company that transacts business with a consumer and then compromises the privacy of consumers' PII has thus deprived that consumer of the full monetary value of the consumer's transaction with the company.

Marriott Failed to Comply with Relevant Industry Standards for Data Security

33. As stated above, Marriott announced on November 30th that a four-years-long data breach had compromised the PII of approximately 500 million Marriott hotel guests worldwide.

34. Marriott claims it discovered the data breach on September 8th when Marriott "received an alert from an internal security tool regarding an attempt to access the Starwood guest reservation database in the United States."[13] Marriott's November 30, 2018 press release further states:

> Marriott quickly engaged leading security experts to help determine what occurred. Marriott learned during the investigation that there had been unauthorized access to the Starwood network since 2014. The company recently discovered that an unauthorized party had copied and encrypted information, and took steps toward removing it. On November 19, 2018, Marriott was able to decrypt the information and determined that the contents were from the Starwood guest reservation database.
>
> The company has not finished identifying duplicate information in the database, but believes it contains information on up to approximately 500 million guests who made a reservation at a Starwood property.
>
> . . .
>
> Marriott reported this incident to law enforcement and continues to support their investigation. The company has already begun notifying regulatory authorities.
>
> "We deeply regret this incident happened," said Arne Sorenson, Marriott's President and Chief Executive Officer. "We fell short of

[13] *Marriott Announces Starwood Guest Reservation Database Security Incident*, MARRIOTT (Nov. 30, 2018), http://news.marriott.com/2018/11/marriott-announces-starwood-guest-reservation-database-security-incident/ (last visited Dec. 4, 2018).

> what our guests deserve and what we expect of ourselves. We are doing everything we can to support our guests, and using lessons learned to be better moving forward."
>
> "Today, Marriott is reaffirming our commitment to our guests around the world. We are working hard to ensure our guests have answers to questions about their personal information, with a dedicated website and call center. We will also continue to support the efforts of law enforcement and to work with leading security experts to improve. Finally, we are devoting the resources necessary to phase out Starwood systems and accelerate the ongoing security enhancements to our network," Mr. Sorenson continued.[14]

35. Plaintiff and Class members often used credit cards to make Marriott reservations. A credit card is a type of payment card. Members of the payment card industry ("PCI") established a Security Standards Counsel ("PCI SSC") in 2006 to develop PCI Data Security Standards ("PCI DSS") for increased security of payment processing systems.

36. The PCI DSS provides: ""PCI DSS applies to all entities involved in payment card processing−including merchants."[15] Marriott is a merchant that accepts payment cards.

37. The PCI DSS requires a merchant to, among other things, protect cardholder data, maintain a vulnerability management program, implement strong access control measures, and regularly monitor and test networks.

38. Furthermore, financial institutions and credit card processing companies have issued rules and standards governing the basic measures that merchants such as Marriott must take to ensure that valuable transactional data is secure and protected. The debit and credit card companies issue regulations ("Card Operating Regulations") that bind Marriott as a condition of its contract with the bank. The Card Operating Regulations prohibit Marriott and other merchants from

[14] *Id.*

[15] *Requirements and Security Assessment Procedures, Version 3.2.1*, Payment Card Industry (PCI) Data Security Standard, at 5 (May 2018), https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-2-1.pdf.

disclosing any card holder account numbers, personal information, or transaction information to third parties (other than the merchant's agent, the acquiring bank, or the acquiring bank's agents). The Card Operating Regulations further require Marriott to maintain the security and confidentiality of debit and credit cardholder information and protect it from unauthorized disclosure.

39. On information and belief, Marriott failed to comply with the PCI DSS as well as Card Operating Regulations, resulting in the Data Breach.

Marriott Failed to Comply with Government Regulations for Data Security

40. Federal and state governments have also created security standards and made recommendations to combat data breaches and the resulting harm to consumers. The FTC has issued several guides for business, emphasizing the importance of reasonable data security practices. According to the FTC, data security should be an element of all business decision-making.[16]

41. According to the FTC, businesses should adhere to the following guidelines for fundamental data security principles and practices for business: protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct security problems.[17] The guidelines also recommend that companies use an intrusion detection system to expose a breach as soon as it happens; monitor all incoming traffic for activity showing that someone is trying to hack the system; look out for large amounts of data being transmitted from the system; and have a response plan ready in case of a breach.[18]

---

[16] *Start With Security, A Guide For Business: Lessons Learned From FTC Cases*, FTC, 2 (April 2007), https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf (last visited Dec. 4, 2018).

[17] *Protecting Personal Information: A Guide For Business*, FTC (October 2016), https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last visited Dec. 4, 2018).

[18] *Id.*

42. The FTC recommends that businesses maintain cardholder information only as long as necessary for authorization of a transaction; limit access to sensitive data; mandate complex passwords to be used on networks; use industry standard security methods; monitor suspicious network activity; and verify that third-party service providers have implemented reasonable security measures.[19]

43. The FTC has brought enforcement actions against companies for failing to adequately protect customer data, treating the failure to employ reasonable and appropriate safeguards to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45. Orders resulting from these actions further illuminate the measures companies must take to comply with their security requirements.

44. Marriott's failure to use reasonable and appropriate procedures to protect against unauthorized access to confidential consumer data comprises an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

45. Marriott was always completely aware of its obligation to protect the PII and financial data of Marriott's guests due to its participation in the storage of PII, storage of payment card information, and interactions with payment card processing networks. Marriott was also cognizant of the major consequences if it failed to do so because Marriott collected payment card data from millions of guests and customers daily and they knew that this data, if hacked, would culminate in harm to consumers, including plaintiff and Class members.

46. Despite Marriott's knowledge of the catastrophic consequences of inadequate data security, Marriott failed to take appropriate protective measures to secure and protect guests' and customers' PII, including plaintiff's and Class members'.

[19] *Start With Security, A Guide For Business: Lessons Learned From FTC Cases*, FTC, *supra*

47. Despite Marriott's knowledge of the catastrophic consequences of inadequate data security, Marriott operated computer network systems with archaic operating systems and software; failed to employ point-to-point and end-to-end encryption; failed to detect intrusions from as far back as 2014; and failed to take other necessary measures to protect its data network.

Damages Sustained By Plaintiff and the Class

48. A portion of the services purchased from Marriott by Plaintiff and the other Class members necessarily included compliance with industry-related measures with respect to the collection and safeguarding of PII, including their credit and debit card information. Because Plaintiff and the Class were denied privacy protections that they paid for and were entitled to receive, Plaintiff and the Class incurred actual monetary damages in that they overpaid for the products and services purchased from Marriott.

49. Plaintiff and the Class have suffered additional injury in fact and actual damages including monetary losses arising from unauthorized bank account withdrawals, fraudulent card payments, and/or related bank fees charged to their accounts.

50. After the Data Breach, Marriott said it was sending email notifications to those who may have been affected and that residents of the United States would be eligible for a free year of enrollment in WebWatcher, an identity fraud alert system. However, as explained above, fraudulent use of cards might not be apparent for years. Therefore, consumers must spend considerable time taking these precautions for years to come.

51. Plaintiff and Class members have a difficult road ahead as a result of the Data Breach. As security blogger Brian Krebs noted while discussing the Michael Stores data breach: "credit monitoring services will do nothing to protect consumers from fraud on existing financial accounts –

---

note 16.

such as credit and debit cards – and they're not great at stopping new account fraud committed in your name."[20]

52. As a result of these activities, Plaintiff and the Class suffered additional damages arising from the costs associated with identity theft and the increased risk of identity theft caused by Marriott's wrongful conduct.

53. Moreover, for customers of credit unions, this breach and the resulting fraud will raise the cost of credit. As one executive at Mission Federal Credit Union noted, because credit unions are non-profits, "when [credit unions] take $100,000 in credit card losses [resulting from fraudulent charges], that's $100,000 that we could have used to give our customers higher interest rates or lower loan rates."[21] Even if a customer is not responsible for fraudulent charges, a data breach resulting in such fraudulent charges will nonetheless raise the cost of acquiring credit by all customers of credit unions, further damaging them.

54. Plaintiff and the Class suffered additional damages based on the opportunity cost and value of time that Plaintiff and the Class have been forced to expend to monitor their financial and bank accounts as a result of the Data Breach. Such damages also include the cost of obtaining replacement and debit cards.

CLASS ACTION ALLEGATIONS

55. Plaintiff brings Count I, as set forth below, on behalf of himself and as a class action, pursuant to the provisions of Rule 23 of the Federal Rules of Civil Procedure on behalf of a class defined as:

---

[20] Brian Krebs, *3 Million Customer Credit, Debit Cards Stolen in Michaels, Aaron Brothers Breaches*, KREBS ON SECURITY (Apr. 14, 2014), https://krebsonsecurity.com/2014/04/3-million-customer-credit-debit-cards-stolen-in-michaels-aaron-brothers-breaches/.

[21] Elizabeth Weise, *Massive data breaches: Where they lead is surprising*, U.S.A. TODAY (Oct. 3, 2014 10:30 AM), https://www.usatoday.com/story/tech/2014/10/02/home-depot-data-breach-

> All persons residing in the United States who provided PII (including payment card information) to Marriott and whose PII was accessed, compromised, or stolen from Marriott in the Data Breach (the "Nationwide Class").

Excluded from the Nationwide Class are Defendant and its affiliates, parents, subsidiaries, employees, officers, agents, and directors. Also excluded is any judicial officer presiding over this matter and the members of their immediate families and judicial staff.

56. Plaintiff brings Count II, as set forth below, on behalf of himself and as a class action, pursuant to the provisions of Rule 23 of the Federal Rules of Civil Procedure on behalf of a class defined as:

> All persons residing in one of the Consumer Fraud States[22] who provided PII (including payment card information) to Marriott and whose PII was accessed, compromised, or stolen from Marriott in the Data Breach (the "Consumer Fraud Multi-State Class").

Excluded from the Consumer Fraud Multi-State Class are Defendant and its affiliates, parents, subsidiaries, employees, officers, agents, and directors. Also excluded is any judicial officer presiding over this matter and the members of their immediate families and judicial staff.

57. The Nationwide Class and the Consumer Fraud Multi-State Class are collectively referred to as the "Class," unless specifically indicated otherwise.

58. Certification of Plaintiff's claims for class-wide treatment is appropriate because Plaintiff can prove the elements of his claims on a class-wide basis using the same evidence as would be used to prove those elements in individual actions alleging the same claims.

---

credit-card-fast-food/16435337/.

[22] The States in the Consumer Fraud Multi-State Class are limited to those States with similar consumer fraud laws under the facts of this case: California (Cal. Bus. & Prof. Code §17200, *et seq.*); Florida (Fla. Stat. §501.201, *et seq.*); Illinois (815 Ill. Comp. Stat. 502/1, *et seq.*); Massachusetts (Mass. Gen. Laws Ch. 93A, *et seq.*); Michigan (Mich. Comp. Laws §445.901, *et seq.*); Minnesota (Minn. Stat. §325F.67, *et seq.*); Missouri (Mo. Rev. Stat. 010, *et seq.*); New Jersey (N.J. Stat. §56:8-1, *et seq.*); New York (N.Y. Gen. Bus. Law §349, *et seq.*); and Washington (Wash.

59. **Numerosity − Federal Rule of Civil Procedure 23(a)(1).** The members of the Class are so numerous that their individual joinder herein is impracticable. On information and belief, there are at least 500 million Class members. The precise number of Class members and their addresses are presently unknown to Plaintiff, but may be ascertained from Marriott's records. Class members may be notified of the pendency of this action by mail, email, Internet postings, and/or publication.

60. **Commonality and Predominance − Federal Rule of Civil Procedure 23(a)(2) and 23(b)(3).** Common questions of law and fact exist as to all Class members and predominate over questions affecting only individual Class members. Such common questions of law or fact include:

a. Whether Marriott failed to use reasonable care and commercially reasonable methods to secure and safeguard its customers' sensitive personal and financial information;

b. Whether Marriott properly implemented its purported security measures to protect customer personal and financial information from unauthorized capture, dissemination, and misuse;

c. Whether Marriott's conduct violates the asserted Consumer Fraud Acts;

d. Whether Marriott's conduct constitutes breach of an implied contract;

e. Whether Plaintiff and the other members of the Class are entitled to damages, injunctive relief, or other equitable relief.

61. Marriott engaged in a common course of conduct giving rise to the legal rights sought to be enforced by Plaintiff, on behalf of himself and the other Class members. Similar or identical statutory and common law violations, business practices, and injuries are involved. Individual

---

Rev. Code §19.86.010, *et seq.*).

questions, if any, pale by comparison, in both quality and quantity, to the numerous common questions that dominate this action.

62. **Typicality − Federal Rule of Civil Procedure 23(a)(3).** Plaintiff's claims are typical of the claims of the other Class members because, among other things, all Class members were comparably injured through Marriott's uniform misconduct described above and were thus all subject to the Data Breach alleged herein. Further, there are no defenses available to Marriott that are unique to Plaintiff.

63. **Adequacy of Representation − Federal Rule of Civil Procedure 23(a)(4).** Plaintiff is an adequate Class representative because his interests do not conflict with the interests of the other Class members he seeks to represent; he has retained counsel competent and experienced in complex class action litigation; and Plaintiff will prosecute this action vigorously. The Class' interests will be fairly and adequately protected by Plaintiff and his counsel.

64. **Insufficiency of Separate Actions − Federal Rule of Civil Procedure 23(b)(1).** Absent a representative class action, members of the Class would continue to suffer the harm described herein, for which they would have no remedy. Even if separate actions could be brought by individual consumers, the resulting multiplicity of lawsuits would cause undue hardship and expense for both the Court and the litigants, as well as create a risk of inconsistent rulings and adjudications that might be dispositive of the interests of similarly situated purchasers, substantially impeding their ability to protect their interests, while establishing incompatible standards of conduct for Marriott. The proposed Class thus satisfies the requirements of Fed. R. Civ. P. 23(b)(1).

65. **Declaratory and Injunctive Relief − Federal Rule of Civil Procedure 23(b)(2).** Marriott has acted or refused to act on grounds generally applicable to Plaintiff and the other Class

members, thereby making appropriate final injunctive relief and declaratory relief, as described below, with respect to the members of the Class as a whole.

66. **Superiority − Federal Rule of Civil Procedure 23(b)(3).** A class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this class action. The damages or other financial detriment suffered by Plaintiff and the other Class members are relatively small compared to the burden and expense that would be required to individually litigate their claims against Marriott, so it would be impracticable for Class members to individually seek redress for Marriott's wrongful conduct. Even if Class members could afford individual litigation, the court system could not. Individualized litigation creates a potential for inconsistent or contradictory judgments, and increases the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties, and provides the benefits of single adjudication, economy of scale, and comprehensive supervision by a single court.

CLAIMS ALLEGED

COUNT I
Breach of Implied Contract
(On Behalf of the National Class)

67. Plaintiff hereby incorporates by reference each paragraph of this Complaint, as if fully set forth herein.

68. Marriott's customers who intended to make reservations were required to provide certain PII as part of the reservation process.

69. In providing such PII, Plaintiff and the other members of the Class entered into an implied contract with Marriott whereby Marriott became obligated to reasonably safeguard Plaintiff's and the other Class members' sensitive, non-public information.

70. Plaintiff and the other Class members would not have entrusted their private and confidential financial and personal information to Defendant in the absence of such an implied contract.

71. Marriott breached the implied contract with Plaintiff and the other members of the Class by failing to take reasonable measures to safeguard their PII.

72. Plaintiff and the other Class members suffered and will continue to suffer damages including, but not limited to loss of their personal and financial information, loss of money, and costs incurred as a result of increased risk of identity theft, all of which have ascertainable value to be proven at trial.

COUNT II
Violation of N.Y. Gen. Bus. Law § 349
(and Substantially Similar Laws of the Consumer Fraud States[23])
(On Behalf of the Consumer Fraud Multi-State Class)

73. Plaintiff hereby incorporates by reference each paragraph of this Complaint, as if fully set forth herein.

74. Defendant's transactions with Plaintiff and the Class are consumer transactions as described herein and constitute the "conduct of any trade or commerce" within the meaning of NYS GBL § 349.

75. Defendant in the normal course of their business collected customer information stating that such data was for the immediate financial transactions.

76. Plaintiff and the other members of the Class were deceived by Marriott's failure to properly implement adequate, commercially reasonable security measures to protect their private personal and financial information while making reservations with Marriott.

[23] The Consumer Fraud States were defined at *supra* note 19.

77. Marriott intended for Plaintiff and the other members of the Class to rely on Marriott to protect the information furnished to it in connection with their reservations, in such manner that the information would be protected, secure, and not susceptible to access from unauthorized third parties.

78. Defendant misrepresented the safety and security of their reservation systems.

79. Marriott instead handled Plaintiff's and the other Class members' personal information in such manner that it was compromised.

80. Marriott failed to follow industry best practices concerning data theft or was negligent in preventing such data theft from occurring.

81. It was foreseeable that Marriott's willful indifference or negligent course of conduct in handling its customers' personal information would put that information at risk of compromise by data thieves.

82. Marriott benefited from mishandling its customers' personal information because, by not taking preventative measures that would have prevented the data from being compromised, Marriott saved on the cost of those security measures.

83. Marriott's fraudulent and deceptive acts and omissions were intended to induce Plaintiff's and the other Class members' reliance on Marriott's deception that their personal and financial information was secure and protected when making reservations with Marriott.[24]

84. The foregoing acts and conduct of Defendant are deceptive in that they represented to the consumer class that such information given to Marriott as part of the reservation process would

[24] The consumer protection statutes or interpretive law of the Consumer Fraud States have also either: (a) expressly prohibited omissions of material fact, without regard for reliance on the deception, or (b) have not addressed those issues.

remain secure and/or that Marriott had the technology or policies to secure personal and financial information when Defendant did not have adequate security measures.

85. The foregoing acts and conduct of Defendant are harmful in that Defendant did not in fact have adequate security in place to secure the financial and sensitive personal information of Plaintiff and the Class.

86. Marriott's acts or practice of failing to employ reasonable and appropriate security measures to protect consumers' personal information constitute violations of the Federal Trade Commission Act, 15 U.S.C. § 45(a).

87. By these deceptive acts, Defendant caused harm to Plaintiff and the Class.

88. Plaintiff's and the other Class members' injuries were proximately caused by Marriott's fraudulent and deceptive behavior, which was conducted with reckless indifference toward the rights of others, such that an award of punitive damages is appropriate.

89. By this conduct, Marriott violated the substantive consumer protection and unfair deceptive trade practices acts or statutes of the Consumer Fraud States, whose laws do not materially differ from that of New York, or conflict with each other for purposes of this action.

JURY TRIAL DEMANDED

Pursuant to Fed. R. Civ. P. 38(b), Plaintiff demands a trial by jury of all the claims asserted.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, individually and on behalf of the other members of the Class proposed in this Complaint, respectfully requests that the Court enter judgment in his favor and against Marriott, as follows:

A. Declaring that this action is a proper class action, certifying the Class as requested herein, designating Plaintiff as Class Representative and appointing the undersigned counsel as Class Counsel for the Class;

B. Ordering Marriott to pay actual damages to Plaintiff and the other members of the Class;

C. Ordering Marriott to pay for not less than three years of credit card monitoring services for Plaintiff and the other members of the Class;

D. Ordering Marriott to pay punitive damages, as allowable by law, to Plaintiff and the other members of the Class;

E. Ordering Marriott to pay statutory damages, as provided by the New York General Business Law § 349 and other applicable State Consumer Fraud Acts, to Plaintiff and the other members of the Class;

F. Ordering Marriott to disseminate individualized notice of the Data Breach to all Class members;

G. Ordering Marriott to pay attorneys' fees and litigation costs to Plaintiff and the other members of the Class;

H. Ordering Marriott to pay both pre- and post-judgment interest on any amounts awarded; and

I. Ordering such other and further relief as may be just and proper.

Dated: December 14, 2018

GLANCY PRONGAY & MURRAY LLP

s/ Brian P. Murray

Brian P. Murray (BM9954)
230 Park Avenue Rm 530
New York, NY 10169
Telephone: (212) 682-5340
Fax: (212) 884-0988
bmurray@glancylaw.com

LAW OFFICE OF PAUL C. WHALEN, P.C.
Paul C. Whalen
768 Plandome Road
Manhasset, NY 11030
Telephone: (516) 426-6870
paul@paulwhalen.com

Attorneys for Plaintiff